Sistema de Acceso y Autenticación en Redes Definidas por Software

Andres Peñasco[1,3], Miguel Méndez-Garabetti[1,2]

[1]Univerisdad de Mendoza, Dirección de Posgrado, Facultad de Ingeniería
penasco.andres@gmail.com, miguel.mendez@um.edu.ar

[2]Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET)

[3]Universidad Nacional de Cuyo, Facultad de Ciencias Aplicadas a la Industria

RESUMEN

Actualmente vivimos en una sociedad digital, donde casi todo está conectado y accesible desde cualquier lugar a través de Internet. Sin embargo, a pesar de su amplia adopción, las redes IP tradicionales de gran envergadura son complejas y muy difíciles de gestionar. Configurar grandes redes según políticas predefinidas, o reconfigurarla para responder a fallas, cambios en la infraestructura y cargas de trabajo, se torna una tarea laboriosa y complicada. Las Redes Definidas por Software (Software-Defined Networking, SDN) son un paradigma emergente que promete mejorar las falencias de las redes convencionales, introduciendo la capacidad de programar la red. Para lograrlo, SDN separa el plano de control del plano de datos, promoviendo la centralización del control de la red y convirtiendo a los routers y switches subyacentes en dispositivos de reenvío de datos simples. Este trabajo de I+D consiste en realizar una revisión bibliográfica de investigaciones recientes, como así también el análisis de los diferentes tipos de soluciones disponibles, incluyendo controladores y tipos de switches, con el objetivo de desarrollar una aplicación que permita administrar el ingreso y la asignación de privilegios de usuarios a una red IP, mediante el uso de flujos manejados por un controlador SDN. De esta forma, será posible demostrar que el desarrollo de aplicaciones que gestionen el plano de control, podrán ofrecer soluciones completas capaces de solucionar los problemas y/o debilidades de las redes tradicionales.

Palabras clave: SDN, openflow, control de acceso, seguridad, redes programables.

CONTEXTO

El presente trabajo de I+D se desarrolla como proyecto se tesis de posgrado de la Maestría en Teleinformática, Dirección de Posgrado, perteneciente a la Facultad de Ingeniería de la Universidad de Mendoza, (Ciudad, Mendoza). El presente proyecto fue aceptado como propuesta de tesis en diciembre de 2016 y aún se encuentra en fase de desarrollo.

1. INTRODUCCIÓN

Las redes de datos se han convertido en uno de los componentes esenciales de toda red

corporativa, siendo de suma importancia que éstas operen de forma eficiente [1]. Por ello, es necesario realizar una adecuada gestión de las redes actuales, considerando la evolución de los sistemas informáticos y las tecnologías emergentes, tales como servicios de computación en la nube [2], sistemas distribuidos [3], Big Data [4], entre otros. En este contexto, las redes de datos tradicionales se enfrentan a una gran cantidad de limitaciones de diseño, que impide la rápida adaptación de la red a cambios, como la reacción ante nuevas vulnerabilidades, implementación de nuevos servicios con requisitos especiales, ampliación de la infraestructura o incorporación de nuevos dispositivos.

Para mantener grandes redes en funcionamiento, es necesario configurar individualmente cada uno de los dispositivos de red, como routers, switches y puntos de acceso, utilizando comandos de bajo nivel, o específicos de cada proveedor. Lo que conlleva un alto grado de complejidad, generando grandes costos operacionales, debido a la especificidad de los conocimientos necesarios para llevar a cabo esta gestión.

Además de la complejidad de configuración mencionada anteriormente, los entornos de red tienen que soportar la dinámica de las fallas y adaptarse a los cambios de carga. En este sentido los mecanismos de reconfiguración y respuesta automática en las redes IP actuales son prácticamente inexistentes. El plano de control (que decide cómo manejar el tráfico de red) y el plano de datos (que reenvía el tráfico de acuerdo con las decisiones tomadas por el plano de control) se agrupan dentro de los dispositivos de red, reduciendo la flexibilidad y obstaculizando la innovación y la evolución de la infraestructura de red. Por ejemplo, la transición de IPv4 a IPv6, iniciada hace más de una década y aún en gran parte incompleta [5], da testimonio de este desafío, mientras que de hecho IPv6 representaba simplemente una actualización de protocolo.

Las redes tradicionales deterministas, que utilizamos hoy en día, en las que el comportamiento de los dispositivos depende de su configuración previa, necesitan evolucionar a una arquitectura de red dinámica, transformándose en entornos escalables, flexibles, fáciles de gestionar y securizar. En respuesta a estas necesidades, se considera que las Redes Definidas por Software (Software-Defined Networking, SDN) [6] y su evolución marcan el camino que ofrece soluciones óptimas a las debilidades planteadas.

Las SDN, son un concepto que viene evolucionando hace varios años y se encuentra en constante desarrollo y expansión. Este tipo de redes divide el plano de datos del plano de control, logrando de esta forma infraestructuras programables, automatizadas, adaptables a las necesidades y problemas futuros [7]. Al separar el plano de control es posible gestionar la red de forma centralizada, gracias a la incorporación de un controlador que mantiene una visión global de la red y del contenido de la misma, proporcionando la capacidad de insertar, modificar o eliminar flujos de datos según sea necesario. Permitiendo programar directamente sobre arquitectura SDN, utilizando módulos de software instalados en el controlador, agilizando los procesos de configuración.

Además, las arquitecturas SDN pueden ser implementadas bajo estándares abiertos, de modo que no dependen de dispositivos de fabricantes específicos o protocolos propietarios. La ONF [8], ha definido el primer estándar abierto, denominado OpenFlow [9], un protocolo que se encuentra en continuo desarrollo y permite manejar directamente el plano de reenvío de dispositivos de red como switches y routers, ya sean físicos o virtuales [7].

Debido a los inconvenientes mencionados de las redes tradicionales, y las ventajas que presenta la arquitectura SDN, es que este trabajo pretende realizar un estudio de la misma, con el propósito de desarrollar un prototipo de aplicación, capaz de gestionar el control de acceso de usuarios en una arquitectura SDN. Para ello se evaluarán los últimos avances registrados en la literatura, tal como los trabajos [10] y [11], donde los autores proponen una solución para el control de acceso a redes en una arquitectura SDN híbrida, utilizando switches virtuales y el protocolo de autenticación RADIUS [12].

El desarrollo aplicación propuesta en este trabajo permitirá administrar el ingreso y la asignación de privilegios de usuarios a la red, mediante el uso de flujos manejados por el controlador SDN. De esta forma, será posible demostrar que el desarrollo de aplicaciones que gestionen el plano de control, permiten ofrecer soluciones completas capaces de solucionar los problemas o debilidades de las redes tradicionales. Además, se realizará un análisis e investigación de diferentes tipos de soluciones disponibles, incluyendo controladores y tipos de switches, como así también la comunicación y configuración de los mismos a través del estándar abierto OpenFlow en sus diferentes versiones.

2. LINEAS DE INVESTIGACIÓN Y DESARROLLO

Redes definidas por software: Se investigará esta tecnología emergente con el objetivo de aplicar las ventajas de la misma, en el desarrollo de la aplicación. Además se analizarán los controladores SDN disponibles para determinar cuál se adapta a las necesidades requeridas por el proyecto.

Protocolos de autenticación: Se realizará un estudio sobre los protocolos y estándares de autenticación existente, tratando de utilizarlos en la aplicación a desarrollar y de este modo brindarle seguridad a la misma.

Virtualización de redes: Se utilizarán herramientas de simulación y virtualización de dispositivos, para generar escenarios de pruebas y poder depurar la aplicación desarrollada antes de utilizarla en un escenario real.

Control de Acceso a redes: Se realizará un análisis de las aplicaciones de control de acceso a redes tradicionales, con el objetivo de comparar ventajas y desventajas con respecto a la aplicación propuesta.

3. RESULTADOS ESPERADOS

El presente proyecto, se centra en el desarrollo e investigación de un método de acceso y autenticación para redes definidas por software, capaz de resolver problemas complejos presentes en las redes actuales.

Particularmente se espera lograr:

1. Estudiar los diferentes tipos de controladores y dispositivos SDN existentes.

2. Evaluar últimos desarrollos e investigaciones realizadas para control de acceso sobre SDN.

3. Implementar una SDN.

4. Configurar y gestionar de forma centralizada los dispositivos de la SDN implementada.

5. Desarrollar un prototipo de aplicación para el control de acceso de usuarios a una arquitectura SDN y evaluar su funcionamiento en contraste con metodologías similares.

6. Documentar características, arquitectura, ventajas y desventajas del protocolo Openflow y las SDN.

7. Evaluar el alcance de la solución y su viabilidad.

4. FORMACIÓN DE RECURSOS HUMANOS

La línea de I+D presentada está vinculada con el desarrollo de una tesis de posgrado por parte del Lic. Andrés Peñasco, quien es estudiante de la Maestría en Teleinformática de la Universidad de Mendoza, la cual tiene como director al Mg. Ing. Miguel Méndez-Garabetti.

5. BIBLIOGRAFÍA

1. W. Stallings, Data and computer communications, 8° ed., Prentice Hall, 2006.

2. NIST, «National Institute of Standards and Technology,» 2011. [En línea]. Disponible: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

3. G. Coulouris, J. Dollimore y T. Kindberg, «Distributed Systems: Concepts and Design,» 5th ed., Addison Wesley, 2011.

4. ISO, «Big Data: Preliminary Report 2014,» 2014. [En línea]. Disponible: http://www.iso.org/iso/big_data_report-jtc1.pdf. [Último acceso: septiembre 2016].

5. O. De León y LACNIC, «Análisis detallado de la información cuantitativa relevante relativa a la transición hacia una red IPv6,» 2014. [En línea]. Disponible: http://portalipv6.lacnic.net/caf-lacnic/anexo-iii/. [Último acceso: Marzo 2016].

6. D. Kreutz, F. Ramos, P. Verissimo, C. Rothenberg, S. Azodolmolky y S. Uhlig, «Software-Defined Networking:A Comprehensive Survey,» IEEE, 2015.

7. Open Networking Foundation, «Software-Defined Networking:The New Norm for Networks,» 2012. [En línea]. Disponible: https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf. [Último acceso: Agosto 2016].

8. Open Networking Foundation, «Software-Defined Networking (SDN) Definition,» 2016. [En línea]. Disponible: https://www.opennetworking.org/sdn-

resources/sdn-definition. [Último acceso: 18 Agosto 2016].

9. N. McKeown, T. Anderson, H. Balakrishnan, P. Guru y L. Peterson, «Openflow,» 2008. [En línea]. Disponible: http://archive.openflow.org/documents/openflow-wp-latest.pdf. [Último acceso: septiembre 2016].

10. V. Dangovas y F. Kuliesius, «SDN-Driven Authentication and Access Control System,» 2014. [En línea]. Disponible: http://sdiwc.net/digital-library/web-admin/upload-pdf/00001098.pdf. [Último acceso: 2016].

11. V. Dangovas y F. Kuliesius, «SDN Enhanced Campus Network Authentication and Access Control System,» 2016. [En línea]. Disponible: http://ieeexplore.ieee.org/document/7536925/. [Último acceso: 10 Septiembre 2016].